REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
22-10-2012	Final Report	1-Nov-2006 - 30-Apr-2013

4. TITLE AND SUBTITLE
Quantum Algorithms - final report

5a. CONTRACT NUMBER
W911NF-07-1-0030

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
411359

6. AUTHORS
Umesh Vazirani

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of California - Berkeley
Sponsored Projects Office
The Regents of the University of California
Berkeley, CA 94704 -5940

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
50602-PH-QC.13

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
We report new directions in which to generalize the success of quantum algorithms. The first gives exponential speedups over classical algorithms for detecting non-linear structures. The algorithm draws its inspiration from optics, where light can be highly focussed when reflected from a conic surface. The second gives a span program based quantum algorithm that achieves quadratic speedup for the evaluation of boolean formulae. The third gives an exponential speedup over classical algorithms for additive approximation to the Tutte polynomial evaluated at

15. SUBJECT TERMS
quantum algorithms, fault tolerance, quantum gap amplification, detectability lemma

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Umesh Vazirani
UU	UU	UU	UU		19b. TELEPHONE NUMBER 510-642-0572

Report Title

Quantum Algorithms - final report

ABSTRACT

We report new directions in which to generalize the success of quantum algorithms. The first gives exponential speedups over classical algorithms for detecting non-linear structures. The algorithm draws its inspiration from optics, where light can be highly focussed when reflected from a conic surface. The second gives a span program based quantum algorithm that achieves quadratic speedup for the evaluation of boolean formulae. The third gives an exponential speedup over classical algorithms for additive approximation to the Tutte polynomial evaluated at certain roots of unity. This leads to an additive approximation of partition functions of statistical mechanics models including the Potts model.

We also report new breakthroughs in fault tolerant quantum computation, based on error detecting codes. And we give an analysis of a Knill type scheme for fault tolerance with a rigorously proved noise threshold of 1/1000.

We introduce a new technique for analyzing local Hamiltonians --- the detectability lemma. We show how to generalize the first step of Dinur's proof of the classical PCP theorem, gap amplification, to the quantum case. Whether or not the quantum PCP theorem is true is a central open question in Hamiltonian complexity.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper	
10/19/2012	3.00	Ben Reichardt. Postselection threshold against biased noise, 2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06). 2006/10/20 03:00:00, Berkeley, CA, USA. : ,
10/19/2012	5.00	Leonard J. Schulman, Andrew M. Childs, Umesh V. Vazirani. Quantum Algorithms for Hidden Nonlinear Structures, 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). 2007/10/20 03:00:00, Providence, RI, USA. : ,
10/19/2012	6.00	Ben W. Reichardt, , Robert Spalek. Span-program-based quantum algorithm for evaluating formulas, Symposium on the theory of computing . 2008/05/17 03:00:00, . : ,
10/19/2012	10.00	Peter Hoyer, Troy Lee, Robert Spalek. Negative weights make adversaries stronger, the thirty-ninth annual ACM symposium. 2007/06/10 03:00:00, San Diego, California, USA. : ,
10/19/2012	11.00	Robert Spalek. The Multiplicative Quantum Adversary, 2008 23rd Annual IEEE Conference on Computational Complexity. 2008/06/22 03:00:00, College Park, MD, USA. : ,
10/19/2012	12.00	Troy Lee, Adi Shraibman, Robert Spalek. A Direct Product Theorem for Discrepancy, 2008 23rd Annual IEEE Conference on Computational Complexity. 2008/06/22 03:00:00, College Park, MD, USA. : ,
TOTAL:	**6**	

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper

TOTAL:

Number of Manuscripts:

Books

Received	Paper

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Ben Reichardt	0.10	
Alexandra Kolla	0.20	
Daniel Preda	0.20	
FTE Equivalent:	**0.50**	
Total Number:	**3**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Rahul Jain	0.20
Robert Spalek	0.20
Jeremy Roland	0.20
FTE Equivalent:	**0.60**
Total Number:	**3**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Umesh Vazirani	0.10	
FTE Equivalent:	**0.10**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME
Ben Reichardt
Alexandra Kolla
Total Number: 2

Names of other research staff

NAME	PERCENT_SUPPORTED
Zeph Landau	0.60
FTE Equivalent:	**0.60**
Total Number:	**1**

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Technology Transfer

Final report on ARO Proposal Number 50602PHQC: "Quantum Algorithms"

Umesh Vazirani

1 Introduction

The search for quantum algorithms that achieve exponential speedups beyond the framework of the hidden subgroup problem is a fundamental challenge in quantum computation. We report three directions for the design of such algorithms. The first is inspired by the fact that the fourier transform interacts well with quadratic surfaces (like parabolic mirrors) to design quantum algorithms for hidden non-linear structures [1]. The second set of algorithms [2,3] are based on the Temperly-Leib algebras and approximations of tensor networks, and yield additive approximations to the Tutte polynomial. These are relevant to estimating quantities of interest in statistical mechanics and in counting complexity. The third gives a span program based quantum algorithm that achieves quadratic speedup for the evaluation of boolean formulae [4].

One of the most important practical obstacles to quantum computers is the difficulty of making the computer robust against environmentally induced decoherence. We report a new, rigorous proof for a Knill type fault-tolerance scheme, based on error detection rather than error correction [5]. The noise threshold of .001 for the scheme that we rigorously establish is considerably better than the best previous bounds using any method. In terms of computational overhead, fault tolerance schemes based on Steane's distance three code are particularly efficient. In [6] we give the first rigorous proof of a noise threshold for a fault tolerant scheme based on a distance three code.

In [7], we introduce a new technique for analyzing local Hamiltonians — the detectability lemma. We show how to generalize the first step of Dinur's proof of the classical PCP theorem, gap amplification, to the quantum case. Whether or not the quantum PCP theorem is true is a central open question in Hamiltonian complexity.

We also report a number of results in quantum complexity theory. In [10] we study Quantum NP further by attempting to generalize the Valiant-Vazirani theorem to the quantum setting. In [11] we report a result showing that honest verifier zero knowledge can be made secure against quantum adversaries. And in [8,9], we explore techniques for proving stronger lower bounds on quantum query complexity.

2 Scientific Progress:

Quantum Algorithms:

The search for quantum algorithms that achieve exponential speedups beyond the framework of the hidden subgroup problem is a fundamental challenge in quantum computation today. The methods that work dramatically, fail equally dramatically for non-abelian groups such as the symmetric group. We report three directions that go beyond the hidden subgroup framework for the design of quantum algorithms.

The first direction [1] starts with shifting the focus back to the Fourier transform over abelian groups, and to consider what other hidden structures can be revealed by abelian Fourier transforms via constructive interference effects. We turn for inspiration to optics and acoustics, where light or sound can be highly focused (i.e., undergo highly constructive interference) when reflected by a conic (e.g., parabolic or elliptic) surface. To connect this idea to known quantum algorithms, observe that

abelian hidden subgroup problems, when restricted to a vector space, can be viewed as determining a hidden linear structure. Any subgroup of the additive group of $\mathcal{F}_q^d$ ($q = p^m$ a prime power) is an $\mathcal{F}_q$-linear subspace, and the cosets of this subgroup consist of parallel affine subspaces, or *flats*. Given a black box function that is constant on each flat and distinct on different ones, abelian Fourier sampling determines the hidden subspace in time $\mathrm{poly}(d \log q)$. Pursuing the analogy with wave mechanics, our approach is to set up black box functions that are constant on quadratic surfaces, and use interference effects to discover properties of the unknown quadratic. More generally, we study this approach for algebraic sets of higher degree.

The first problem we study is the *hidden radius problem*. In this problem, the hidden property is the radius r of a sphere. We give an efficient quantum algorithm for determining one bit of r, namely whether or not it is a quadratic residue, assuming that the dimension is odd. With a classical computation, even this restricted problem requires exponentially many queries. (For the problem of determining the other bits of r, we argue that the quantum query complexity is small.)

The second problem we consider is the *hidden flat of centers problem*. In this problem, the radius of the sphere is fixed (say, at $r = 1$), but its center is constrained to lie in an unknown flat in $\mathcal{F}_q^d$. For example, the centers of the spheres may lie on an unknown line. For this problem, we give an efficient quantum algorithm to determine the entire hidden flat, not just one bit of information about it. However, this algorithm also works only when the dimension is odd. The main idea of the algorithm is to use a quantum walk to move amplitude from the spheres to their centers. Our algorithms for both this and the hidden radius problem make crucial use of a connection to certain exponential sums called *twisted Kloosterman sums*.

Both of the above problems fall into a framework of *shifted subset problems*. For problems in this class, the main idea is to define a black box function that is constant on some subset of the points in $\mathcal{F}q^d$, as well as on shifted versions of this subset, with the function taking distinct values when the shifts are different. The goal may be either to determine some property of the basic subset, or of the allowed shifts, or both. Typically, this will not give a well-defined black box, since different shifts of the subset may lead to overlapping points. However, we can resolve this issue by defining the black box carefully.

Assuming the degree of $h(x)$ is constant, we show that the query complexity of the hidden polynomial problem is typically $\mathrm{poly}(\log q)$. We show this by considering an analog of the standard approach to the HSP, wherein one query of the black box is used to produce a quantum state that depends on the hidden object. Provided these states are sufficiently statistically distinguishable, it follows that $\mathrm{poly}(\log q)$ copies contain enough information to determine the hidden object with high probability.

The second direction, reported in [2,3], relies on the representation theory for the Temperley-Lieb algebras to design new quantum algorithms for a combinatorial/topological question. This is a radical new direction for quantum algorithms, since it breaks from the use of the quantum Fourier transform as the main computational ingredient. We list a few features of the new algorithms below:

1. The works provide new quantum algorithm for the combinatorial/topological question of additively approximating two important structures: the Tutte polynomial (and consequently the Potts model which is a specialization of the Tutte polynomial) and the partition function of various statistical mechanical models.

2. The works show that for certain parameters, additive approximation of both the Tutte polynomial and the partition function of the statistical mechanical models are complete problems for quantum computation.

3. Perhaps most remarkably, the works are able to move away from the unitary paradigm that quantum computation is cast in. Specifically, both the approximating algorithms and the completeness results hold for parameters where the relevant operators are not unitary. This demonstrates that a quantum computer can be used to address problems that don't seem to have a

unitary component.

4. The main tool for [2] is the representation theory for the Temperley-Lieb algebras. The main tool for [3] are the realization of the quantities of interest as the evaluation of tensor networks. Collectively, this is a completely new direction for quantum algorithms which, for the most part, have used the quantum Fourier transform as the main computational ingredient.

The third direction [4] builds on the breakthrough result of Farhi, Goldstone and Gutman, to give a quantum algorithm for evaluating formulas over an extended gate set, including all two- and three-bit binary gates (e.g., NAND, 3-majority). The algorithm is optimal on read-once formulas for which each gate's inputs are balanced in a certain sense. The main new tool is a correspondence between a classical linear-algebraic model of computation, "span programs," and weighted bipartite graphs. A span program's evaluation corresponds to an eigenvalue-zero eigenvector of the associated graph. A quantum computer can therefore evaluate the span program by applying spectral estimation to the graph. For example, the classical complexity of evaluating the balanced ternary majority formula is unknown, and the natural generalization of randomized alpha-beta pruning is known to be suboptimal. In contrast, our algorithm generalizes the optimal quantum AND-OR formula evaluation algorithm and is optimal for evaluating the balanced ternary majority formula.

Fault-tolerance Bounds:

The value of the quantum noise threshold, or maximum tolerable gate error rate allowing reliable quantum computation, together with the overhead required to attain it, are of considerable experimental interest.

The highest current estimates for the amount of noise a quantum computer can tolerate are based on fault-tolerance schemes relying heavily on postselecting on no detected errors. In particular, Knill has constructed a novel fault-tolerance scheme based on very e?cient distance-two codes. Being of distance two, his codes allow for error detection, not correction, and the scheme uses extensive postselection on no detected errors i.e., on detecting an error, the enclosing subroutine is restarted. Knill has estimated that the threshold for his scheme is perhaps as high as 3-6%. However, there has been no rigorous proof that any scheme based on postselection gives even a positive tolerable noise threshold. In [5], we report a technique to prove a positive threshold, for probabilistic noise models. The main idea is to maintain strong control over the distribution of errors in the quantum state at all times. This distribution has correlations which conceivably could grow out of control with postselection. But in fact, the error distribution can be written as a mixture of nearby distributions each satisfying strong independence properties, so there are no correlations for postselection to amplify. Indeed, with some more care we are able to rigorously establish a noise threshold of .001, an order of magnitude improvement upon earlier bounds using other schemes.

In terms of actual computational overhead, the most efficient quantum fault tolerance schemes are designed using the Steane seven-qubit, distance-three quantum code. This is no doubt because its elegant simplicity, and its small size allows for easy, efficient simulations. Although noise thresholds are frequently estimated for such fault tolerance schemes, there has been no proof that a constant threshold even exists for distance-three codes. In [6], we prove the existence of a constant threshold. The proven threshold is well below estimates, based on simulations and analytic models, of the true threshold, but at least it is now known to be positive.

Quantum PCP theorem

One of the most important results in classical theoretical computer science is the PCP theorem, which states the following counter intuitive fact: proofs (or solutions to computational problems in

the complexity class NP) can be cast into such a form that their correctness can be verified by looking at only 3 (!) bits of the proof. The impact of this result on computer science has been unmeasureable.

To transition to its quantum analogue, it is useful to think of a classical PCP as a constraint satisfaction problem, such that either all contraints are satisfiable or a constant fraction must be violated. The quantum analogue of a constraint satisfaction problem is the local Hamiltonian problem, with the ground energy providing the quantum analogue of the number of violated constraints. So the natural quantum analogue of the PCP theorem would assert that any sum of local Hamiltonians may be mapped to a new robust local Hamiltonian system such that if the ground energy of the original system was 0 it remains so, but if it was slightly larger than 0 then it is amplified to a constant.

The possible implications of a quantum PCP theorem are of utmost significance. To begin with, just as in the classical setting, a quantum PCP theorem would have implications regarding the hardness of approximate solutions on quantum computers. Second, using the connection drawn in the work of Aharonov et al between adiabatic computations and the k-local Hamiltonian problem, it is likely that a quantum PCP theorem might lead to a fault tolerant quantum adiabatic theorem, thus solving a major open question. Thirdly, a quantum PCP theorem is likely to have interesting implications towards the understanding of ground states and ground energies of local Hamiltonians. Most importantly, the attempts to generalize the PCP proof to the quantum world touch upon fundamental issues in quantum mechanics: the meaning of the no-cloning theorem, and the nature of entanglement. The PCP proof in the classical case (in particular the simplest recent proof by Dinur) relies heavily on the possibility to copy bits, which is impossible in the quantum world due to the no-cloning theorem. This does not rule out a quantum PCP theorem, since as we point out in [7], there is a doubly exponential sized quantum PCP. The main issue is whether a quantum PCP of reasonable complexity can be realized. Any answer is likely to shed light on the fundamental notions of entanglement and no-cloning.

We propose to study whether or not the PCP theorem has a classical analog. In the positive direction, we start with Dinur's combinatorial proof of the PCP theorem. Dinur's proof consists of an iteration of a three step process: preprocessing, gap amplification and alphabet reduction. We report in [7] that one interesting step in Dinur's proof of the PCP theorem, namely the gap amplifiction can be carried out in a quantum setting. The result is non-trivial, and we sketch it below:

The quantum analog of a constraint satisfaction problem is a sum of local Hamiltonians - each (term of the) Hamiltonian specifies a local constraint whose violation contributes to the energy of the given quantum state. Formalizing the intuitive connection between the ground (minimal) energy of the Hamiltonian and the *minimum* number of violated constraints is problematic, since the number of constraints being violated is not well defined when the terms in the Hamiltonian do not commute. The paper starts by establishing the detectability lemma, which provides precisely such a quantitative connection. Assuming that each particle participates in a bounded number of terms of the Hamiltonian, the terms can be decomposed into a constant number of layers such that all the terms within a layer commute with each other. Thus it makes sense to speak about the number of violated constraints in a given layer. The detectability lemma asserts that the probability that there is a term of the Hamiltonian in a random layer that is violated is proportional to the energy of the ground state. The detectability lemma can be used to establish the quantum analog of gap amplification.

Finally, at the technical core of the detectability lemma lies the XY decomposition, which appears interesting in its own right as a technique for understanding the ground states of local Hamiltonians. Very roughly, the XY decomposition partitions the Hilbert space into a tensor product of local spaces and then further decomposes each of these local spaces into commuting (X) and non-commuting parts (Y) with respect to the Hamiltonian. This allows for a local analysis of the actions of the individual terms of the Hamiltonian, the result of which is a parameter for which these actions can be shown to have exponential decay when restricted to the non-commuting part of the decomposition. A potential application of the lemma is to resolve the quantum complexity of finding the ground state of a local Hamiltonian, where all the terms of the Hamiltonian commute.

Quantum complexity theory:

The quantum adversary method is one of the most successful techniques for proving lower bounds on quantum query complexity. It gives optimal lower bounds for many problems, has application to classical complexity in formula size lower bounds, and is versatile with equivalent formulations in terms of weight schemes, eigenvalues, and Kolmogorov complexity. All these formulations are information-theoretic and rely on the principle that if an algorithm successfully computes a function then, in particular, it is able to distinguish between inputs which map to different values.

We present a stronger version of the adversary method which goes beyond this principle to make explicit use of the stronger condition that the algorithm actually computes the function[8]. This new method, which we call ADV, has all the advantages of the old: it is a lower bound on bounded-error quantum query complexity, its square is a lower bound on formula size, and it behaves well with respect to function composition. Moreover ADV is always at least as large as the adversary method ADV, and we show an example of a monotone function for which $ADV(f) = \Omega(ADV(f)^{1.098})$. We also give examples showing that ADV does not face limitations of ADV such as the certificate complexity barrier and the property testing barrier.

In [9], we present a new variant of the quantum adversary method. All adversary methods give lower bounds on the quantum query complexity of a function by bounding the change of a progress function caused by one query. All previous variants upper-bound the di?erence of the progress function, whereas our new variant upper-bounds the ratio and that is why we coin it the multiplicative adversary. The new method generalizes to all functions the new quantum lower-bound method by Ambainis based on the analysis of eigenspaces of the density matrix. We prove a strong direct product theorem for all functions that have a multiplicative adversary lower bound.

In [10] we study Quantum NP further by attempting to generalize the Valiant-Vazirani theorem to the quantum setting. This theorem states that the complexity of problems in NP remain (almost) unchanged even under the promise that the solution is unique; the quantum analogue would read "if the ground state is unique". We prove the analogue of the Valiant-Vazirani theorem for the probabilistic version of NP, namely, MA, as well as for the class QCMA, which is defined like QMA except the witness is classical. The result implies that one cannot expect efficient descriptions of the sort of MPSs for one dimensional Hamiltonians with inverse polynomial gap, (unless QCMA=NP, which is believed to be unlikely). Unfortunately and surprisingly, we prove that the straightforward generalization of the proof fails for QMA. It is also unclear whether oracle separations such as those used by Aaronson and Kuperberg to separate QCMA from QMA can be useful here to imply a separation. Whether Unique-QMA equals QMA is left as an intriguing open problem, with implications to to the physical question of the possibility of removing redundancy of local Hamiltonians.

Let L be a language decided by a constant-round quantum Arthur-Merlin (QAM) protocol with negligible soundness error and all but possibly the last message being classical. In [11] we prove that if this protocol is zero knowledge with a black-box, quantum simulator S, then $L \in BQP$. Our result also applies to any language having a three-round quantum interactive proof (QIP), with all but possibly the last message being classical, with negligible soundness error and a black-box quantum simulator. These results in particular make it unlikely that certain protocols can be composed in parallel in order to reduce soundness error, while maintaining zero knowledge with a black-box quantum simulator. They generalize analogous classical results of Goldreich and Krawczyk (1990). Our proof goes via a reduction to quantum black-box search. We show that the existence of a black-box quantum simulator for such protocols when $L \notin BQP$ would imply an impossibly-good quantum search algorithm.

Bibliography:

[1] Childs,, Andrew M. and Schulman,, Leonard J. and Vazirani,, Umesh V., "Quantum Algorithms for Hidden Nonlinear Structures," Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, 2007, pages 395-404.

[2] Aharonov, D. and Arad, I. and Eban, E. and Landau, Z., "Polynomial Quantum Algorithms for Additive approximations of the Potts model and other Points of the Tutte Plane," Arxiv preprint quant-ph/0702008, 2007.

[3] Arad, I. and Landau, Z., "Quantum computation and the evaluation of tensor networks," arXiv:0805.0040 [quant-ph], 2008.

[4] Ben Reichardt, Robert Spalek, "Span-program-based quantum algorithm for evaluating formulas", arXiv:0710.2630 [quant-ph], 2007.

[5] Ben Reichardt, "Postselection threshold against biased noise," Symposium on the Foundations of Computer Science, 2006.

[6] Ben Reichardt, "Fault-Tolerance Threshold for a Distance-Three Quantum Code", Lecture Notes in Computer Science, Springer, ISN 0302-9743, Volume 4051/2006, 2006, Pages 50-61.

[7] Aharonov, D., Arad, I., Landau, Z., and Vazirani, U. The detectability lemma and quantum gap amplification. In Proceedings of the 41st Annual ACM Symposium on theory of Computing (Bethesda, MD, USA, May 31 - June 02, 2009). STOC '09. ACM, New York, NY, 417-426.

[8] Hoyer,, Peter and Lee,, Troy and Spalek,, Robert, "Negative weights make adversaries stronger," Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, 2007, pages 526–535.

[9] Spalek, R., "The Multiplicative Quantum Adversary," arXiv:quant-ph/0703237, 2007.

[10] Dorit Aharonov, Michael Ben-Or, Fernando G.S.L. Brandao, Or Sattath, "The Pursuit For Uniqueness: Extending Valiant-Vazirani Theorem to the Probabilistic and Quantum Settings," arXiv:0810.4840 [quant-ph], 2008.

[11] Rahul Jain, Alexandra Kolla, Gatis Midrijanis, and Ben Reichardt. "On parallel composition of zero-knowledge proofs with black-box quantum simulators," Quantum Information and Computation, 2006.